



Dockets Management Staff (HFA-105)
U.S. Food and Drug Administration
5630 Fishers Lane
Room 1061,
Rockville, MD 20852

July 7, 2022

Re: Docket No. FDA-2021-D-1158; Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions Draft Guidance for Industry and Food and Drug Administration Staff

IAMERS¹ appreciates the opportunity to comment on “Cybersecurity In Medical Devices: Quality System Considerations and Content of Premarket Submissions”, Docket No. FDA-2021-D-1158. IAMERS commends the U.S. Food and Drug Administration’s efforts to promote transparency and to offer best practices consistent within applicable law. IAMERS continues to be aligned with the FDA as to the need for cybersecurity for medical devices and in particular, the need for cybersecurity for legacy medical devices.

IAMERS welcomes the amount and level of detailed information contemplated by this new draft guidance.² Patient safety and management of potential risks mandate that users and servicers have access to appropriate information. Efforts to limit this information to only that deemed by the OEM to be appropriate could potentially jeopardize the ability of users and servicers to address undisclosed cybersecurity vulnerabilities.³ Some manufacturers seem to be motivated to limit their sharing of information in order to preserve the financial benefit of an

¹ International Association of Medical Equipment Remarketers and Servicers, Inc. (“IAMERS”).

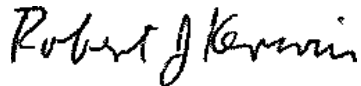
² For example, the section entitled “IC, Transparency at 6, lines 194-206.

³ In 2021, the FTC, following a hearing entitled ‘Nixing the Fix’, issued a report to Congress and observed manufacturers do not always cooperate in providing instructions for repair. <https://www.ftc.gov/reports/nixing-fix-ftc-report-congress-repair-restrictions>.

exclusive service arrangement with the user. Manufacturers so motivated often claim that information should not be shared because it could compromise cybersecurity, or it could encourage service by unqualified personnel. As the draft Guidance acknowledges: “[t]his information and other relevant information is important in helping understand a device’s cybersecurity, the threats that it may be exposed to, and how those threats may be prevented or mitigated.” Usually, the users and their technical support personnel are in the best position to understand, analyze and mitigate the cybersecurity risks associated with the operation of the device in their unique ecosystem.

If you have any questions, please feel free to contact me directly, rkerwin@iamers.org.

Very truly yours,



Robert J. Kerwin
IAMERS General Counsel

Cc: Ms. Diana Upton, IAMERS President